UNITED STATES PATENT AND TRADEMARK OFFICE

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/071,873	02/08/2002	James Richmond	E00378.70179/JHM/DPM	8737

23628	7590	03/08/2004

WOLF GREENFIELD & SACKS, PC
FEDERAL RESERVE PLAZA
600 ATLANTIC AVENUE
BOSTON, MA 02210-2211

EXAMINER
REVAK, CHRISTOPHER A

ART UNIT	PAPER NUMBER
2131	6

DATE MAILED: 03/08/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

PTO-90C (Rev. 10/03)

	Application No.	**Applicant(s)**
Office Action Summary	10/071,873	RICHMOND ET AL.
	Examiner	**Art Unit**	
	Christopher A. Revak	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE <u>3</u> MONTH(S) FROM
THE MAILING DATE OF THIS COMMUNICATION.
- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed
  after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
  Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any
  earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *17 December 2003*.
2a)☒ This action is **FINAL**.   2b)☐ This action is non-final.
3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is
     closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-46* is/are pending in the application.
    4a) Of the above claim(s) _____ is/are withdrawn from consideration.
5)☐ Claim(s) _____ is/are allowed.
6)☒ Claim(s) *1-46* is/are rejected.
7)☐ Claim(s) _____ is/are objected to.
8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.
10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.
     Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
     Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
    a)☐ All   b)☐ Some * c)☐ None of:
      1.☐ Certified copies of the priority documents have been received.
      2.☐ Certified copies of the priority documents have been received in Application No. _____.
      3.☐ Copies of the certified copies of the priority documents have been received in this National Stage
           application from the International Bureau (PCT Rule 17.2(a)).
    * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
   Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413)
   Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Response to Arguments

1.   Applicant's arguments filed on December 17, 2003 have been fully considered but they are not persuasive.

It is argued by the applicant that Nessett fails to disclose of a user having an assigned role with respect to the network, but rather recites of implementing a device specific specific policy. The examiner agrees and it is noted in the rejection that the teachings of Nessett fail to disclose of a user being assigned a role with respect to the network, please refer to the rejection as is recited below. In response to applicant's arguments against the references individually, one cannot show nonobviousness by attacking references individually where the rejections are based on combinations of references. See *In re Keller*, 642 F.2d 413, 208 USPQ 871 (CCPA 1981); *In re Merck & Co.*, 800 F.2d 1091, 231 USPQ 375 (Fed. Cir. 1986).

It is additionally argued by the applicant that Dixon fails to disclose of determining the role of a user with respect to a network or configuring a port module of a network device based on a determined role. The examiner respectfully disagrees for it is disclosed by Dixon of an authority context based on an underlying policy and provides authority for particular types of traffic from that user and user interface (port module) and allows a user to define its own access control (paragraph 11). The user policy is configured to a device that is directly connected to the network (as shown in Figure 4 and as recited on page 13, claim 21).

In response to applicant's argument that there is no suggestion to combine the references, the examiner recognizes that obviousness can only be established by combining or modifying the teachings of the prior art to produce the claimed invention where there is some teaching, suggestion, or motivation to do so found either in the references themselves or in the knowledge generally available to one of ordinary skill in the art. See *In re Fine*, 837 F.2d 1071, 5 USPQ2d 1596 (Fed. Cir. 1988)and *In re Jones*, 958 F.2d 347, 21 USPQ2d 1941 (Fed. Cir. 1992). In this case, Dixon et al recites motivation for use of this concept by teaching that prior art security protocols in distributed firewalls provide authentication only at a machine level (page 1, paragraph 10, lines 3-4) and the teachings of Dixon et al solve that problem by authenticating individual users and not individual machines whereby the prior art has no means of knowing when a plurality of different users are accessing a secure machine to gain access to network resources (page 2, paragraph 10, lines 9-14).

The applicant has additionally argued that it is not taught of a computer program product comprising a computer readable medium and computer readable signals stored on the computer readable medium that define instructions that, as a result of being executed by a computer, instruct the computer. The examiner respectfully disagrees and the applicant makes a mere assertion that of these limitations not being taught. The examiner has taken official notice that these limitations are notoriously well known. The applicant has failed to seasonably traverse the examiner's assertion of official notice and has not adequately traversed such a finding by specifically pointing out the

supposed errors in the examiner's action, which would include stating why the noticed fact is not considered to be common knowledge or well-known in the art.

Claim Rejections - 35 USC § 103

1.   The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

2.   Claims 1-46 are rejected under 35 U.S.C. 103(a) as being unpatentable over Nessett et al in view of Dixon et al.

As per claims 1,17,33,35,40, and 45, it is disclosed by Nessett et al of distributing firewall functionality into network devices such as network cards which include a policy definition component that accepts (configures) policy data (packet rules) that define how the firewall should behave (column 3, lines 22-27,29-34). Nessett et al disclosed that the network interface cards are attached to an end system through it internal I/O bus (port module) and provides access (entry point) to a Local Area Network (column 11, lines 25-28). The user is authenticated prior to granting authorization (based on the packet rules) to access resources from the Internet (column 15, lines 43-46). The teachings of Nessett et al disclose of authenticating a user prior to granting access to use resources (column 15, lines 41-46), but are silent in disclosing of configuring packet rules corresponding to the identity of a user and the use of a port module. It is disclosed by Dixon et al of authenticating a user (to establish their identity) and then

establishing a user security context (rules) for traffic (packet) for a user and once

authenticated, provides authorization based on the security context for that user. Dixon

additionally recites of an authority context based on an underlying policy and provides

authority for particular types of traffic from that user and user interface (port module)

and allows a user to define its own access control (page 1, paragraph 11). The user

policy is configured to a device that is directly connected to the network (as shown in

Figure 4 and as recited on page 13, claim 21). It would have been obvious to a person

of ordinary skill in the art at the time of the invention to have been motivated to apply the

teachings of Dixon et al as a means of a distributed firewall pertaining to a specific user.

Dixon et al recites motivation for use of this concept by teaching that prior art security

protocols in distributed firewalls provide authentication only at a machine level (page 1,

paragraph 10, lines 3-4) and the teachings of Dixon et al solve that problem by

authenticating individual users and not individual machines whereby the prior art has no

means of knowing when a plurality of different users are accessing a secure machine to

gain access to network resources (page 2, paragraph 10, lines 9-14). It would have

been obvious that the teachings of Nessett et al would have benefited from the

motivation of Dixon et al as a means of authenticating a particular user and not the

actual device as is taught by Dixon et al.

As per claims 2,18,39, and 44, it is disclosed by Dixon et al of authenticating a

user prior to granting authorization (page 1, paragraph 11, lines 1-5). The examiner

supplies the same rationale for the motivation as recited in the rejection of claims

1,17,33,35, and 40 to modify the teachings of Nessett et al.

As per claims 3,4,19, and 20, the teachings of Nessett et al disclose of
distributing firewall functionality into network devices such as network cards which
include a policy definition component that accepts (configures) policy data (packet rules)
that define how the firewall should behave (column 3, lines 22-27,29-34). Dixon et al is
relied upon for authenticating a user (to establish their identity) and then establishing a
user security context (rules) for traffic (packet) for a user and once authenticated,
provides authorization based on the security context for that user (page 1, paragraph
11, lines 1-5). The examiner supplies the same rationale for the motivation as recited in
the rejection of claims 1,17,33,35, and 40 to modify the teachings of Nessett et al. The
combination of the teachings of Nessett et al and Dixon et al are silent in disclosing of
applying the packet rules until a user logs off the communication network. The
examiner hereby takes official notice that packet rules until a user logs off the
communication network are notoriously well known. It would have been obvious to a
person of ordinary skill in the art at the time of the invention that it is known to close
sessions and corresponding rules applying to that session once a user has logged off
the communication network. It is notoriously well known that a security feature of
closing security features once a user has logged off a communications network is a
common feature which protects the integrity of a security policy when a user is not
currently logged in and active. By requiring a user to relog-in, the security policy
(packet rules) is re-instated based upon re-entry of a user into the system which would
protect the integrity of the security policy against an unauthorized user from gaining
access to the security policy (packet rules) when they are not properly authenticated

and authorized to participate in the security policy. It is obvious that the combined

teachings of Nessett et al and Dixon et al would have used the concept of applying the

packet rules until a user logs off the communication network.

As per claims 5-7,21-23,37,38,42, and 43, it is disclosed by Nessett et al of

distributing firewall functionality into network devices such as network cards which

include a policy definition component that accepts (configures) policy data (packet rules)

that define how the firewall should behave (column 3, lines 22-27,29-34). Nessett et al

disclosed that the network interface cards are attached to an end system through it

internal I/O bus (port module) and provides access (entry point) to a Local Area Network

(column 11, lines 25-28). Dixon et al is relied upon for authenticating a user (to

establish their identity) and then establishing a user security context (rules) for traffic

(packet) for a user and once authenticated, provides authorization based on the security

context for that user (page 1, paragraph 11, lines 1-5). The user authentication and

application/purpose (identity and role) is provided (page 2, paragraph 13, lines 2-3).

The examiner supplies the same rationale for the motivation as recited in the rejection

of claims 1,17,33,35, and 40 to modify the teachings of Nessett et al.

As per claims 8 and 24, Nessett et al discloses of distributing firewall functionality

into network devices such as network cards and routers (for routing packets) which

include a policy definition component that accepts (configures) policy data (packet rules)

that define how the firewall should behave (column 3, lines 22-27,29-34).

As per claims 9 and 25, Nessett et al discloses of filtering packets and dropping them based on the values in their headers (column 1, lines 20-23) based on the policy (packet rules)(column 3, lines 22-27,29-34).

As per claims 10-12 and 26-28, Nessett et al discloses of making changes to the network topology (which includes packet creation/modification/adding) and requires the policy data to be reconfigured (column 17, line 65 through column 18, line 5).

As per claims 13 and 29, the combined teachings of Nessett et al and Dixon et al are silent in disclosing of controlling the amount of bandwidth consumed by a user. The examiner hereby takes official notice that the use of controlling bandwidth is notoriously well known. It would have been obvious to a person of ordinary skill in the art at the time of the invention to be motivated to apply bandwidth consumption measures on a user. It is notoriously well known that high bandwidth consumption can affect the operations of a network. It is known that high bandwidth consumption by transferring large amounts of data restricts other's ability to transfer data since only there exists a threshold of the amount of data that can be transferred. By restricting the amount of bandwidth a user is entitled to, it allows an equal opportunity to other users to allow sharing of the available bandwidth whereby one user can not use the majority of the bandwidth by themselves. It is obvious that the combined teachings of Nessett et al and Dixon et al would have used this feature of limiting bandwidth to users so that all users have an equal opportunity to transfer information.

As per claims 14-16 and 30-32, Nessett et al discloses of distributing firewall functionality into network devices such as network cards which include a policy

·definition component that accepts (configures) policy data (packet rules) that define how

the firewall should behave (controlling access to devices and resources/applications)

(column 3, lines 22-27,29-34). Nessett et al disclosed that the network interface cards

are attached to an end system through it internal I/O bus (port module) and provides

access (entry point) to a Local Area Network (column 11, lines 25-28). The user is-

authenticated prior to granting authorization (based on the packet rules) to access

resources from the Internet (column 15, lines 43-46).

As per claims 34 and 46, it is disclosed by Nessett et al of distributing firewall

functionality into network devices such as network cards which include a policy

definition component that accepts (configures) policy data (packet rules) that define how

the firewall should behave (column 3, lines 22-27,29-34). Nessett et al disclosed that

the network interface cards are attached to an end system through it internal I/O bus

(port module) and provides access (entry point) to a Local Area Network (column 11,

lines 25-28). The user is authenticated prior to granting authorization (based on the

packet rules) to access resources from the Internet (column 15, lines 43-46). The

teachings of Nessett et al is silent in disclosing of a computer program product

comprising a computer-readable medium and computer-signals stored on the computer-

readable medium that define instructions when executed by a computer to instruct the

computer to perform the process. The examiner hereby takes official notice that it

would have been obvious to a person of ordinary skill in the art that the teachings of

Nessett et al comprise a memory for storing computer readable code and a processor

coupled to memory that is configured to execute the computer readable code in order

for the teachings to be performed as disclosed. The software program (computer

readable code) and necessary hardware (processor and memory) to perform the

necessary tasks are notoriously known to one of skill in the art as an essential part of

computing. It is obvious that the teachings Nessett et al exist in the form of a software

program (computer readable code) and are utilized by the hardware, namely stored in

memory and a processor interprets, processes, and performs the task of enforcing a

distributed firewall in a network device such as a network interface card.

The teachings of Nessett et al disclose of authenticating a user prior to granting

access to use resources (column 15, lines 41-46), but are silent in disclosing of

configuring packet rules corresponding to the identity of a user and the use of a port

module. It is disclosed by Dixon et al of authenticating a user (to establish their identity)

and then establishing a user security context (rules) for traffic (packet) for a user and

once authenticated, provides authorization based on the security context for that user.

Dixon additionally recites of an authority context based on an underlying policy and

provides authority for particular types of traffic from that user and user interface (port

module) and allows a user to define its own access control (page 1, paragraph 11). The

user policy is configured to a device that is directly connected to the network (as shown

in Figure 4 and as recited on page 13, claim 21). It would have been obvious to a

person of ordinary skill in the art at the time of the invention to have been motivated to

apply the teachings of Dixon et al as a means of a distributed firewall pertaining to a

specific user. Dixon et al recites motivation for use of this concept by teaching that prior

art security protocols in distributed firewalls provide authentication only at a machine

level (page 1, paragraph 10, lines 3-4) and the teachings of Dixon et al solve that

problem by authenticating individual users and not individual machines whereby the

prior art has no means of knowing when a plurality of different users are accessing a

secure machine to gain access to network resources (page 2, paragraph 10, lines 9-14).

It would have been obvious that the teachings of Nessett et al would have benefited

from the motivation of Dixon et al as a means of authenticating a particular user and not

the actual device as is taught by Dixon et al.

As per claims 36 and 41, Nessett et al discloses that the network interface cards

are attached to an end system through it internal I/O bus (port module) and provides

access (entry point) to a Local Area Network (column 11, lines 25-28).

Conclusion

3.   Applicant's amendment necessitated the new ground(s) of rejection presented in

this Office action. Accordingly, **THIS ACTION IS MADE FINAL.** See MPEP

§ 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37

CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE

MONTHS from the mailing date of this action. In the event a first reply is filed within

TWO MONTHS of the mailing date of this final action and the advisory action is not

mailed until after the end of the THREE-MONTH shortened statutory period, then the

shortened statutory period will expire on the date the advisory action is mailed, and any

extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of

the advisory action. In no event, however, will the statutory period for reply expire later

than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the

examiner should be directed to Christopher A. Revak whose telephone number is 703-

305-1843. The examiner can normally be reached on Monday-Friday, 6:30am-4:00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's

supervisor, Ayaz Sheikh can be reached on 703-305-9648. The fax phone number for

the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the

Patent Application Information Retrieval (PAIR) system. Status information for

published applications may be obtained from either Private PAIR or Public PAIR.

Status information for unpublished applications is available through Private PAIR only.

For more information about the PAIR system, see http://pair-direct.uspto.gov. Should

you have questions on access to the Private PAIR system, contact the Electronic

Business Center (EBC) at 866-217-9197 (toll-free).

CR

March 4, 2004

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100